IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application: **Adler et al.**	§	Group Art Unit: **3621**
	§	
	§	
Serial No.: **09/884,296**	§	Examiner: **Fischer, Andrew J.**
	§	
Filed: **June 19, 2001**	§	Attorney Docket No.: **AUS920010620US1**
	§	
For: **Using a Privacy Agreement Framework to Improve Handling of Personally Identifiable Information**	§	Customer No. **50170**
	§	
	§	

REPLY TO NEW GROUND OF REJECTION IN EXAMINER'S ANSWER

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

No fees are believed to be required. If, however, any fees are required, I authorize the Commissioner to charge these fees which may be required to IBM Corporation Deposit Account No. 09-0447. No extension of time is believed to be necessary. If, however, an extension of time is required, the extension is requested, and I authorize the Commissioner to charge any fees for this extension to IBM Corporation Deposit Account No. 09-0447.

In response to the new ground of rejection set forth in the Examiner's Answer mailed December 9, 2008, and further to the Request to Re-Open Prosecution filed herewith, please amend the above-identified application as follows:

Listing of Claims begins on page 2 of this paper.

Remarks begin on page 9 of this paper.

CLAIMS:

1. (Currently amended) A method, in an information handling system comprising a processor and a storage device, for improving the handling of personally identifiable information, said method comprising:

generating, in the information handling system, an object model for representing relationships between active entities with regard to handling of personally identifiable information, wherein the active entities comprise a data subject, represented as a data subject object in the object model, and at least one data user, represented as at least one data user object in the object model, and wherein the data subject is an active entity that is identified by the personally identifiable information and the at least one data user is an active entity that uses the personally identifiable information obtained from the data subject;

identifying [[the]], by the information handling system, parties involved in a process of handling personally identifiable information based on the object model, wherein the parties comprise the data subject and the at least one data user;

identifying, by the information handling system, [[the]] data involved in said process from a data model;

classifying, by the information handling system, the data as personally identifiable information or non-personally identifiable information;

expressing, by the information handling system, based on the object model, each relationship between each pair of said parties in terms of a privacy agreement, wherein the privacy agreement for each relationship between each pair of parties is a subset of a natural language privacy policy set, the subset being defined as specific to a particular situation or purpose and specific to the particular parties in the pair of parties; and

representing, by the information handling system, said parties, said data, and said privacy agreements graphically as objects and associations between objects in one or more privacy agreement relationship diagrams, wherein:

[[said]] each privacy agreement uses a limited number of privacy-related actions concerning said personally identifiable information; and

said privacy agreement expresses privacy rules regarding said privacy-related actions, for each ~~of said parties~~ party in a pair of parties with which the privacy agreement is associated~~; and~~

~~said privacy agreement is specific to a single purpose~~.

2. (Currently amended) The method of Claim 1, further comprising mapping a business process to [[the]] privacy rules ~~that should govern the behavior~~ of one or more privacy agreements for each pair of parties.

3. (Currently amended) The method of Claim 1, further comprising identifying opportunities to reduce privacy-related risks involved in said process based on the one or more privacy agreement relationship diagrams.

4. (Currently amended) The method of Claim 3, further comprising identifying unnecessary exchanges of data, for possible elimination based on the one or more privacy agreement relationship diagrams.

5. (Currently amended) The method of Claim 3, further comprising identifying opportunities to transform data into a less sensitive form based on the one or more privacy agreement relationship diagrams, wherein the less sensitive form is one of a de-personalized form or an anonymous form.

6. (Currently amended) A system for improving the handling of personally identifiable information, said system comprising:

a processor; and

a memory coupled to the processor, wherein the memory comprises instructions which, when executed by the processor, cause the processor to:

generate an object model for representing relationships between active entities with regard to handling of personally identifiable information, wherein the active entities comprise a data subject, represented as a data subject object in the object model, and at least one data user, represented as at least one data user object in the object model, and

wherein the data subject is an active entity that is identified by the personally identifiable information and the at least one data user is an active entity that uses the personally identifiable information obtained from the data subject;

~~means for identifying the~~ identify parties involved in a process of handling personally identifiable information based on the object model, wherein the parties comprise the data subject and the at least one data user;

~~means for identifying the~~ identify data involved in said process from a data model;

~~means for classifying~~ classify the data as personally identifiable information or non-personally identifiable information;

~~means for expressing~~ express, based on the object model, each relationship between each pair of said parties in terms of a privacy agreement, wherein the privacy agreement for each relationship between each pair of parties is a subset of a natural language privacy policy set, the subset being defined as specific to a particular situation or purpose and specific to the particular parties in the pair of parties; and

~~means for representing~~ represent said parties, said data, and said privacy agreements graphically as objects and associations between objects in one or more privacy agreement relationship diagrams, wherein:

[[said]] each privacy agreement uses a limited number of privacy-related actions concerning said personally identifiable information; and

said privacy agreement expresses privacy rules regarding said privacy-related actions, for each ~~of said parties~~ party in a pair of parties with which the privacy agreement is associated~~; and~~

~~said privacy agreement is specific to a single purpose~~.

7. (Currently amended) The system of Claim 6, ~~further comprising means for mapping~~ wherein the instructions further cause the processor to map a business process to [[the]] privacy rules ~~that should govern the behavior~~ of one or more privacy agreements for each pair of parties.

8. (Currently amended) The system of Claim 6, ~~further comprising means for identifying~~ wherein the instructions further cause the processor to identify opportunities to reduce privacy-related risks involved in said process based on the one or more privacy agreement relationship diagrams.

9. (Currently amended) The system of Claim 8, ~~further comprising means for identifying~~ wherein the instructions further cause the processor to identify unnecessary exchanges of data, for possible elimination based on the one or more privacy agreement relationship diagrams.

10. (Currently amended) The system of Claim 8, ~~further comprising means for identifying~~ wherein the instructions further cause the processor to identify opportunities to transform data into a less sensitive form based on the one or more privacy agreement relationship diagrams, wherein the less sensitive form is one of a de-personalized form or an anonymous form.

11. (Currently amended) A computer-usable medium having computer-executable instructions for improving the handling of personally identifiable information, said computer-executable instructions ~~comprising~~, when executed by a computing device, cause the computing device to:

generate an object model for representing relationships between active entities with regard to handling of personally identifiable information, wherein the active entities comprise a data subject, represented as a data subject object in the object model, and at least one data user, represented as at least one data user object in the object model, and wherein the data subject is an active entity that is identified by the personally identifiable information and the at least one data user is an active entity that uses the personally identifiable information obtained from the data subject;

~~means for identifying the~~ identify parties involved in a process of handling personally identifiable information based on the object model, wherein the parties comprise the data subject and the at least one data user;

~~means for identifying the~~ identify data involved in said process from a data model;

~~means for classifying~~ classify the data as personally identifiable information or non-personally identifiable information;

~~means for expressing~~ express, based on the object model, each relationship between each pair of said parties in terms of a privacy agreement, wherein the privacy agreement for each relationship between each pair of parties is a subset of a natural language privacy policy set, the subset being defined as specific to a particular situation or purpose and specific to the particular parties in the pair of parties; and

~~means for representing~~ represent said parties, said data, and said privacy agreements graphically as objects and associations between objects in one or more privacy agreement relationship diagrams, wherein:

[[said]] each privacy agreement uses a limited number of privacy-related actions concerning said personally identifiable information; and

said privacy agreement expresses privacy rules regarding said privacy-related actions, for each ~~of said parties~~ party in a pair of parties with which the privacy agreement is associated~~; and~~

~~said privacy agreement is specific to a single purpose~~.

12. (Currently amended) The computer-useable medium of Claim 11, ~~further comprising means for mapping~~ wherein the instructions further cause the computing device to map a business process to [[the]] privacy rules ~~that should govern the behavior~~ of one or more privacy agreements for each pair of parties.

13. (Currently amended) The computer-useable medium of Claim 11, ~~further comprising means for identifying~~ wherein the instructions further cause the computing device to identify opportunities to reduce privacy-related risks involved in said process based on the one or more privacy agreement relationship diagrams.

14. (Currently amended) The computer-useable medium of Claim 13, ~~further comprising means for identifying~~ wherein the instructions further cause the computing

device to identify unnecessary exchanges of data, for possible elimination based on the one or more privacy agreement relationship diagrams.

15. (Currently amended) The computer-useable medium of Claim 13, ~~further comprising means for identifying~~ wherein the instructions further cause the computing device to identify opportunities to transform data into a less sensitive form based on the one or more privacy agreement relationship diagrams, wherein the less sensitive form is one of a de-personalized form or an anonymous form.

16. (New) The method of Claim 5, wherein the less sensitive form is a de-personalized form in which transformed data does not contain personally identifiable information that identifies the data subject but is able to be associated with the data subject using other data having personally identifiable information.

17. (New) The method of Claim 5, wherein the less sensitive form is an anonymous form in which transformed data does not contain personally identifiable information that identifiers the data subject and is not able to be associated with the data subject.

18. (New) The system of Claim 10, wherein the less sensitive form is a de-personalized form in which transformed data does not contain personally identifiable information that identifies the data subject but is able to be associated with the data subject using other data having personally identifiable information.

19. (New) The system of Claim 10, wherein the less sensitive form is an anonymous form in which transformed data does not contain personally identifiable information that identifiers the data subject and is not able to be associated with the data subject.

20. (New) The computer-useable medium of Claim 15, wherein the de-personalized form is a form in which transformed data does not contain personally identifiable information that identifies the data subject but is able to be associated with the data subject using other data having personally identifiable information, and wherein the

anonymous form is a form in which transformed data does not contain personally identifiable information that identifiers the data subject and is not able to be associated with the data subject.

REMARKS

Claims 1-20 are pending in the present application. By this Reply to the New Ground of Rejection in the Examiner's Answer, claims 1-15 are amended and claims 16-20 are added. Independent claim 1 is amended in light of the new ground of rejection to tie the method to another statutory class of invention, namely an information handling system having a processor and a storage device. Independent claims 1, 6 and 11 are amended to further emphasize and clarify the distinctions of the present invention over the cited references. The amendments to claims 1, 6, and 11 are supported by the present specification at least in paragraphs [0087] to [0090] (referring to the corresponding application publication no. 2003/0014418) and in Figures 5-7. Amendments to dependent claims 2-5, 7-10, and 12-15 are to make these claims consistent with the amendments to the respective independent claims. Moreover, claims 5, 10, and 15 are amended to clarify that the less sensitive form is one of a de-personalized form or an anonymous form. Claims 16-20 are added to further define what is meant by the terms de-personalized form and anonymous form.

Entry of these amendments is proper under MPEP § 1207.03(V)(A) since the present reply includes amendments addressing the new ground of rejection set forth in the Examiner's Answer along with additional amendments which are appropriate under this section (MPEP § 1207.03(V)(A) states "the reply may also include amendments, evidence, and/or arguments directed to claims not subject to the new ground of rejection or other rejections"). No new matter has been added by any of the above amendments or addition of new claims. Reconsideration of the claims is respectfully requested in view of the following remarks.

I. Rejections Set Forth in Examiner's Answer

The Examiner's Answer sets forth the following rejections of the claims:

(1) Claims 1, 2, 6, 7, 11, and 12 are rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over King (EP 1,081,916 A2) in view of Kroenke,

"Database Processing: Fundamentals, Design, and Implementation," copyright 1999;

(2) Claims 3-5, 8-10, and 13-15 are rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over King in view of Kroenke, and further in view of Spies et al. (U.S. Patent No. 5,689,565); and

(3) Claims 1-5 are rejected under 35 U.S.C. § 101 as being allegedly directed to non-statutory subject matter based on the *In re Bilski* decision, 88 USPQ2d 1385 (Fed. Cir. 2008) (en banc).

Rejection (3) in the above constitutes a new rejection and is the basis for the request to re-open prosecution of this application. Each of these rejections is addressed herein below.

II. Rejection under 35 U.S.C. § 101

With regard to the rejection of claims 1-5 under 35 U.S.C. § 101, by this Reply, Applicants have amended claim 1 to clearly tie the method recited in the claim to another statutory class of invention. In particular, claim 1 is amended to recite that the method is performed in an information handling system that comprises a processor and a storage device. As a result, claim 1, and its dependent claims, positively recite the machine that accomplishes the method steps. Thus, the claims cannot be interpreted as being purely a mental process. Therefore, amended claims 1-5 are directed to statutory subject matter at least because they satisfy the first prong of the two prong test set forth in the Examiner's Answer. Accordingly, Applicants respectfully request withdrawal of the rejection of claims 1-5 under 35 U.S.C. § 101.

III. Rejection Under 35 U.S.C. § 103(a) Based on King and Kroenke

With regard to the rejection of claims 1, 2, 6, 7, 11, and 12 under 35 U.S.C. § 103(a), Applicants first respectfully direct the Examiner's attention to the arguments presented in the Appeal Brief filed December 4, 2004, the Reply Brief filed March 7,

2005, and the Reply Brief filed June 13, 2006 as Applicants believe that these arguments are still applicable to the pending claims. The arguments set forth in the Appeal Brief and Reply Briefs are hereby incorporated by reference.

The main point to recognize from these arguments is that neither the King nor Kroenke reference, either alone or in combination, teaches or provides any technical rationale to implement representing the entities, data and relationships between entities, of a process of handling personally identifiable information, graphically as one or more privacy agreement relationship diagrams. In addition, Applicants submitted that there is no teaching or technical rationale to combine and modify the King and Kroenke references to arrive at the claimed invention.

In addition to the points raised in the Appeal Brief and Reply Briefs, Applicants have further emphasized the differences between the claimed invention and the King and Kroenke references by the amendments made in this Reply. Taking amended claim 1 as representative of the other independent claims 6 and 11, with regard to similarly recited subject matter, claim 1 recites:

> 1. (Currently amended) A method, in an information handling system comprising a processor and a storage device, for improving the handling of personally identifiable information, said method comprising:
>
> generating, in the information handling system, an object model for representing relationships between active entities with regard to handling of personally identifiable information, wherein the active entities comprise a data subject, represented as a data subject object in the object model, and at least one data user, represented as at least one data user object in the object model, and wherein the data subject is an active entity that is identified by the personally identifiable information and the at least one data user is an active entity that uses the personally identifiable information obtained from the data subject;
>
> identifying, by the information handling system, parties involved in a process of handling personally identifiable information based on the object model, wherein the parties comprise the data subject and the at least one data user;
>
> identifying, by the information handling system, data involved in said process from a data model;
>
> classifying, by the information handling system, the data as personally identifiable information or non-personally identifiable information;

expressing, by the information handling system, based on the object model, each relationship between each pair of said parties in terms of a privacy agreement, wherein the privacy agreement for each relationship between each pair of parties is a subset of a natural language privacy policy set, the subset being defined as specific to a particular situation or purpose and specific to the particular parties in the pair of parties; and

representing, by the information handling system, said parties, said data, and said privacy agreements graphically as objects and associations between objects in one or more privacy agreement relationship diagrams, wherein:

each privacy agreement uses a limited number of privacy-related actions concerning said personally identifiable information; and

said privacy agreement expresses privacy rules regarding said privacy-related actions, for each party in a pair of parties with which the privacy agreement is associated. (emphasis added)

Applicants respectfully submit that neither King nor Kroenke, either alone or in combination, teach or provide any technical rationale to implement, the features of claim 1 emphasized above or the similar features found in the other independent claims 6 and 11.

King is directed to a system and method for controlling the transfer of sensitive information between a client device and a server device based on established privacy agreements between the client device and the server device. With the system and method of King, a proxy device is operatively connected between a wireless client device and a server device to manage distribution of private information. The proxy server device has a storage area to store the private information and a privacy manager which operates to restrict the release of the information to other server devices unless a suitable privacy agreement governing the use of the information is in place.

King does not teach or provide any technical rationale to implement, generating an object model for representing relationships between active entities with regard to handling of personally identifiable information, wherein the active entities comprise a data subject, represented as a data subject object in the object model, and at least one data user, represented as at least one data user object in the object model, and wherein the data subject is an active entity that is identified by the personally identifiable information and the at least one data user is an active entity that uses the personally identifiable

information obtained from the data subject, as recited in claim 1. Nowhere in King is there any mention of an object model, let alone the generation of such an object model that has a data subject object and a data user object.

In addition, King does not teach or provide any technical rationale regarding the identification of parties involved in a process of handling personally identifiable information based on the object model, wherein the parties comprise the data subject and the at least one data user. Again, there is no object model in King and thus, King cannot be found to teach the identification of parties in a process of handling personally identifiable information based on such an object model.

Furthermore, King does not teach or provide any technical rationale regarding classifying data obtained from a data model as personally identifiable information or non-personally identifiable information. While King controls the release of private information, King does not classify data obtained from a data model based on whether that information is personally identifiable information or non-personally identifiable information.

Moreover, King does not teach or provide any technical rationale regarding expressing, based on an object model, each relationship between each pair of parties in terms of a privacy agreement, wherein the privacy agreement for each relationship between each pair of parties is a subset of a natural language privacy policy set, the subset being defined as specific to a particular situation or purpose and specific to the particular parties in the pair of parties, as recited in claim 1. King mentions a privacy agreement needing to be in place in order for private information to be released. However, nowhere does King teach or even allude to expressing relationships between parties as privacy agreements that are subsets of a natural language privacy policy set that are defined as specific to a particular situation or purpose and specific to the particular parties in the pair of parties.

In addition to all of the above, King does not teach or provide any technical rationale to represent the parties, the data, and the privacy agreements graphically as objects and associations between objects in one or more privacy agreement relationship diagrams. Again, while King mentions privacy agreements and using them to control the transfer of information, nowhere in King is there any teaching or even technical rationale

provided to represent parties, data, and privacy agreements graphically in one or more privacy agreement relationship diagrams. The Examiner does not contest this lack of teaching in King and in fact admits that King lacks such teachings. However, contrary to the Examiner's allegations, Kroenke does not teach or provide any technical rationale to include these features either.

Kroenke is a general textbook describing database processing, and happens to have a section directed to entity-relationship modeling using a database schema. A number of diagrams are shown for illustrative purposes to explain examples of relationships between entities that may be represented in a database schema. While these diagrams are present in the textbook of Kroenke, these diagrams are merely illustrative of examples for explaining the entity relationship model and do not teach or even suggest to generate privacy agreement relationship diagrams to represent parties, data and privacy agreements of a process of handling personally identifiable information. That is, while Kroenke provides diagrams of relationships between entities for explanation of a database schema, there is no actual teaching in Kroenke to take data of a process for handling personally identifiable information, information regarding relationships between pairs of parties in a privacy agreement, and representing this information in a graphical form as one or more privacy agreement relationship diagrams. Thus, neither Kroenke nor King, either taken alone or in combination, teach or provide any technical rationale to represent parties, data and privacy agreements graphically as objects and associations between objects in one or more privacy agreement relationship diagrams, as recited in claims 1, 6 and 11.

Moreover, Kroenke does not provide any teaching or technical rationale to incorporate any of the other features lacking in King as discussed above. Nowhere in Kroenke is there any teaching or technical rationale to include a system such as taught by King any of the features of generating an object model for representing relationships between active entities with regard to handling of personally identifiable information, identifying parties involved in a process of handling personally identifiable information based on the object model, classifying data obtained from a data model as personally identifiable information or non-personally identifiable information, expressing, based on an object model, each relationship between each pair of parties in terms of a privacy

agreement, or representing parties, data, and privacy agreements graphically as objects and associations between objects in one or more privacy agreement relationship diagrams, in the manner specifically recited in the independent claims. Therefore, any alleged combination of Kroenke and King, even though such a combination would not be possible and is not reasonable for the reasons set forth previously in the Appeal Brief and Reply Briefs (which are incorporated herein by reference), still would not result in the specific combination of features set forth in claims 1, 6, and 11 being taught or rendered obvious.

Furthermore, as discussed at length in Applicants' Appeal and Reply Briefs, King and Kroenke are not directed to solving a similar problem using computer implemented methods, despite the allegations made by the Examiner. King is concerned with controlling the transfer of sensitive information between a client device and a server device by using privacy agreements. Kroenke describes a database schema that may be used with the entity-relationship model. These are not the same problem. In fact, there is no discernable problem addressed by Kroenke. Kroenke merely provides an explanation of a database schema. Thus, the Examiner's allegation that King and Kroenke are directed to solving the same problem is erroneous and not supported by the actual teachings of the references.

The Examiner states that the reason to combine the King and Kroenke references is present in the references at least at paragraph 007 of King and pages 59+ of Kroenke because both make reference to Business Rules. Appellants have reviewed paragraph 007 of King and do not find any reference to "business rules" in this paragraph of the reference. What is stated is that the exchange of sensitive information may be governed by one or more privacy agreements established between the principle parties, i.e. a client device and a server device. King also states in this paragraph that a proxy server can manage a list of realms that are allowed sensitive information and may be used to negotiate privacy agreements. However, nowhere in this section of King is there any mention of "business rules" as alleged by the Examiner.

At page 59+, the Kroenke reference describes a database schema that consists of tables, relationships, domains and business rules. The business rules are added to the database schema during a data modeling stage. While Kroenke teaches the inclusion of

business rules in a database schema, this does not provide any teaching or technical rationale to combine Kroenke with King.

Moreover, the Examiner's statement that because both references may mention business rules, that somehow they now become combinable, is also a mistaken attempt to support a combination of teachings from non-analogous references. Merely mentioning business rules and that business rules may be added to the database schema in Kroenke does not give any teaching or technical rationale to combine Kroenke with King. Many different systems may make use of business rules and yet not be combinable with the system and method described in King. The mere mention of business rules in some later section of Kroenke does not provide any teaching or technical rationale to combine the concept of generating relationship diagrams, allegedly taught by Kroenke although Appellants disagree for the reasons stated above, with the teachings of King. To the contrary, the Examiner's pointing to "business rules" as a way of linking the references is a mere attempt to support a combination that is based on two non-analogous references that do not provide any motivation to combine their features by finding any possible commonality regardless of how irrelevant it is to the features that are allegedly being combined.

Thus, Applicants respectfully submit that independent claims 1, 6, and 11 are distinguished over the alleged combination of King and Kroenke. At least by virtue of their dependency on claims 1, 6, and 11, respectively, dependent claims 2, 7, and 12 are likewise distinguished over the alleged combination of King and Kroenke. Accordingly, Applicants respectfully request withdrawal of the rejection of claims 1, 2, 6, 7, 11, and 12 under 35 U.S.C. § 103(a).

IV. Rejection Under 35 U.S.C. § 103(a) Based on King, Kroenke and Spies

With regard to the rejection of claims 3-5, 8-10 and 13-15 under 35 U.S.C. § 103(a), these dependent claims are distinguished over the alleged combination of references at least for the same reasons as noted above with regard to claims 1, 6 and 11. The Spies reference does not provide any teaching or technical rationale to cure the deficiencies noted above with regard to King and Kroenke. Spies teaches yet another

field of technology – encryption. Thus, in the rejections of claims 3-5, 8-10 and 13-15, not only is the Examiner attempting to combine the non-analogous King and Kroenke references, but is now adding a third reference, Spies, that is directed to a completely different area of technology than King and Kroenke.

Merely because Spies may generally teach to mitigate risk associated with personal, sensitive information by reducing or restricting access to this information, this general teaching does not render the specific features recited in the dependent claims 3-5, 8-10 and 13-15 unpatentable. To the contrary, Spies teaches a specific way in which to reduce access to information – encryption. Nowhere in Spies is there any teaching or technical rationale to identify opportunities to reduce privacy-related risks involved in a process of handling personally identifiable information based on one or more privacy agreement relationship diagrams, as recited in claim 3. Moreover, nowhere in Spies is there any teaching or technical rationale to identify unnecessary exchanges of data based on one or more privacy agreement relationship diagrams, as recited in claim 4, or identifying opportunities to transform data into a less sensitive format based on one or more privacy agreement relationship diagrams, as recited in claim 5. The Examiner merely states that these features are obvious because Spies gives a general concept that one would want to reduce access to information in order to mitigate risk. The Examiner is using a general concept to reject specific features. The general concept does not obviate all specific implementations of the general concept and thus, the general concept in this case does not obviate the specific features recited in claims 3-5, 8-10 and 13-15. The fact is, the references simply do not teach or provide any technical rationale to implement the specific features recited in these claims, despite the allegations made by the Examiner regarding the general goal of reducing access to information in order to mitigate risk.

In view of the above, Applicants respectfully submit that claims 3-5, 8-10, and 13-15 are distinguished over the alleged combination of King, Kroenke, and Spies. Accordingly, Applicants respectfully request withdrawal of the rejection of claims 3-5, 8-10, and 13-15 under 35 U.S.C. § 103(a).

V. Newly Added Claims

Claims 16-20 are added to further define the less sensitive forms of data referenced in dependent claims 5, 10, and 15. None of the cited references, either alone or in combination, teach or provide any technical rationale to implement either a de-personalized form of data or anonymous data form as recited in these claims, respectively. Thus, in addition to the various reasons set forth above with regard to the claims from which they depend, claims 16-20 also recite additional features for which there is no teaching or technical rationale provided in the King, Kroenke, and Spies references.

VI. Conclusion

It is respectfully urged that the subject application is now in condition for allowance. The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

Respectfully submitted,

DATE: February 5, 2009

Stephen J. Walder, Jr.
Reg. No. 41,534
WALDER INTELLECTUAL PROPERTY LAW, P.C.
17330 Preston Road, Suite 100B
Dallas, TX 75252
(972) 380-9475
ATTORNEY FOR APPLICANTS